09/869816
PCT/JP00/07728
02.11.00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

KU

REC'D 17 NOV 2000
WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

JP00/7728

出願年月日
Date of Application: １９９９年１１月 ５日

出願番号
Application Number: 平成１１年特許願第３１４８８０号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２０００年 ９月 １日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０６９９６３

【書類名】　特許願

【整理番号】　9900843008

【提出日】　平成11年11月 5日

【あて先】　特許庁長官　近藤　隆彦　殿

【国際特許分類】　G06F　1/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　猪口　達也

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐古　曜一郎

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082762

【弁理士】

【氏名又は名称】　杉浦　正知

【電話番号】　03-3980-0339

【手数料の表示】

【予納台帳番号】　043812

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708843

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　データ復号装置および方法、課金情報処理装置および方法、並びにデータ再生装置および方法

【特許請求の範囲】

【請求項１】　符号化または暗号化されたディジタルデータを復号する復号装置において、

符号化または暗号化されたディジタルデータを復号する復号手段と、

視聴権データを記憶するための記憶手段と、

上記符号化または暗号化されたデータを復号する際に、上記ディジタルデータに付随されている再生条件情報の指示に従って上記記憶手段内の上記視聴権データに変更を加えることにより課金処理を行う課金制御手段とを備えたことを特徴とするデータ復号装置。

【請求項２】　請求項１において、

復号したディジタルデータの識別子および／または復号の条件を記憶するための記憶手段を有し、

上記ディジタルデータの復号時に上記記憶手段にログを残すことを特徴とするデータ復号装置。

【請求項３】　請求項１において、

データを暗号化することによって、外部の特定の機器との間で安全にデータ交換できるインターフェースを有し、上記インターフェースを介して上記記憶手段に視聴権データを格納できることを特徴とするデータ復号装置。

【請求項４】　請求項１において、

データを暗号化することによって、外部の特定の機器との間で安全にデータ交換できるインターフェースを有し、上記インターフェースを介して上記記憶手段内のログデータを出力または入力または変更できることを特徴とするデータ復号装置。

【請求項５】　請求項３または４において、

上記インターフェースが非接触通信手段を備えていることを特徴とするデータ復号装置。

【請求項６】　請求項５において、

上記インターフェースが電力受信手段を備えており、

本体の電源が供給されていない状況においても上記インターフェースを介して上記記憶手段内のデータにアクセスできることを特徴とするデータ復号装置。

【請求項７】　請求項１において、

データを復号した際に、上記再生条件情報の一部または全部、または上記再生条件情報のデータにある演算を施した結果を、復号が可能なウォーターマークとして出力データに埋め込むことを特徴とするデータ復号装置。

【請求項８】　請求項１において、

データを復号した際に、ウォーターマークが付加されている場合は、上記ウォーターマークに埋め込まれたデータを復号し、再生条件情報から得られる正規の値と等しい場合のみ復号データを出力することを特徴とするデータ復号装置。

【請求項９】　符号化または暗号化されたディジタルデータを復号する復号方法において、

符号化または暗号化されたディジタルデータを復号するステップと、

上記符号化または暗号化されたデータを復号する際に、上記ディジタルデータに付随されている再生条件情報の指示に従って記憶されている視聴権データに変更を加えることにより課金処理を行うステップとを備えたことを特徴とするデータ復号方法。

【請求項１０】　決裁センターとデータ復号装置との間で、視聴権データを中継するための課金情報処理装置において、

複数のデータ復号装置の間で共用可能なように、可搬型とされたことを特徴とする課金情報処理装置。

【請求項１１】　決裁センターとデータ復号装置との間で、視聴権データを中継するための課金情報処理装置において、

有線または無線通信手段を介して決裁センターに直接または他の機器を中継して接続できる通信手段と、

上記決裁センターから安全に視聴権データを得るための手段と、

上記視聴権データを記憶する記憶手段と、

外部の機器との間で安全に視聴権データの一部または全部を転送するための手段を有するインターフェースとからなることを特徴とする課金情報処理装置。

【請求項１２】　請求項１０または１１において、

上記通信手段は、電話線或いはインターネットに直接または他の機器を中継して接続可能であることを特徴とする課金情報処理装置。

【請求項１３】　請求項１０または１１において、

使用状況を記録したログを記憶するための記憶手段を有し、

上記インターフェースを介して上記記憶手段から外部の機器に対して視聴権データを転送する際に、上記外部の機器から使用状況を記録したログを上記記憶手段に転送することを特徴とする課金情報処理装置。

【請求項１４】　請求項１０または１１において、

上記決裁センターと接続した際に、決裁センターで決裁済みの視聴権データを上記記憶手段に転送すると同時に、上記記憶手段に蓄積されている使用状況を記録したログを上記決裁センターに転送することを特徴とする課金情報処理装置。

【請求項１５】　請求項１０または１１において、

上記インターフェースが非接触通信手段を備えていることを特徴とする課金情報処理装置。

【請求項１６】　請求項１０または１１において、

上記インターフェースを通じて課金情報処理装置間で視聴権データの一部または全部を移動・合算・分割可能とされたことを特徴とする課金情報処理装置。

【請求項１７】　決裁センターとデータ復号装置との間で、視聴権データを中継するための課金情報処理装置において、

外部の機器との間で安全に視聴権データの一部または全部を転送するための手段を有するインターフェースと、

上記視聴権データを記憶する記憶手段とを備え、

上記インターフェースは、ＩＣカードとの間で上記視聴権データの転送が可能なことを特徴とする課金情報処理装置。

【請求項１８】　請求項１７において、

使用状況を記録したログを記憶するための記憶手段を有し、

上記インターフェースを介して上記記憶手段から外部の機器に対して視聴権データを転送する際に、上記外部の機器から使用状況を記録したログを上記記憶手段に転送することを特徴とする課金情報処理装置。

【請求項１９】　請求項１７において、

ＩＣカードから視聴権データを上記記憶手段に転送すると同時に、上記記憶手段に蓄積されている使用状況を記録したログをＩＣカードに転送することを特徴とする課金情報処理装置。

【請求項２０】　請求項１７において、

上記インターフェースが非接触通信手段を備えていることを特徴とする課金情報処理装置。

【請求項２１】　決裁センターとデータ復号装置との間で、視聴権データを中継するための課金情報処理方法において、

有線または無線通信手段を介して決裁センターに直接または他の機器を中継して接続するステップと、

上記決裁センターから安全に視聴権データを得るステップと、

上記視聴権データを記憶するステップと、

外部の機器との間で安全に視聴権データの一部または全部を転送するステップとからなることを特徴とする課金情報処理方法。

【請求項２２】　圧縮符号化および／または暗号化されたディジタルデータを再生するデータ再生装置において、

上記ディジタルデータを復号する復号装置を備え、

上記復号装置は、

符号化または暗号化されたディジタルデータを復号する復号手段と、

視聴権データを記憶するための記憶手段と、

上記符号化または暗号化されたデータを復号する際に、上記ディジタルデータに付随されている再生条件情報の指示に従って上記記憶手段内の上記視聴権データに変更を加えることにより課金処理を行う課金制御手段とを備えたことを特徴とするデータ再生装置。

【請求項２３】　圧縮符号化および／または暗号化されたディジタルデータを再生するデータ再生方法において、

符号化または暗号化されたディジタルデータを復号するステップと、

上記符号化または暗号化されたデータを復号する際に、上記ディジタルデータに付随されている再生条件情報の指示に従って記憶されている視聴権データに変更を加えることにより課金処理を行うステップとを備えたことを特徴とするデータ再生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えば音楽配信に適用されるデータ復号装置および方法、課金情報処理装置および方法、並びにデータ再生装置および方法に関する。

【０００２】

【従来の技術】

コンパクトディスク(Compact Disc;ＣＤ)、ＤＶＤ (Digital Versatile Disc または Digital Video Disc) 等において、著作権保護のために、違法なコピーを防止するためのコピー防止技術が種々提案され、また、実用化されている。例えばＳＣＭＳ(Serial Copy Management System) は、ＣＤからＭＤ (Mini Disc)への１世代目のコピーを許可しても、ＭＤから他の媒体への２世代目のコピーを禁止するものである。また、何世代目のコピーを作成できるかを制限するコピー世代制限の方式も知られている。

【０００３】

一方、最近では、インターネットを始めとする急速なネットワークの発展の下で、ネットワークを介して音楽コンテンツが流通するようになってきている。そのような状況において、インターネット、衛星放送等のネットワークを利用したＥＭＤ(Electronic Music Distribution) が開始され、ＥＭＤにおける著作権管理の方法が提案されている。ＥＭＤにおいては、課金によってユーザが音楽コンテンツを入手することができる。このＥＭＤにおいても、違法コピーを防止するために上述したようなＳＣＭＳ、コピー世代制限等の技術が使用されようとして

いる。

【０００４】

上述したように、従来の著作権保護の方法は、コピー防止技術を用いてコピーを制限し、著作権者の権利を保護するものであったために、音楽コンテンツを広く、且つ短時間に流通させる上では、障害となっていた。例えば従来の著作権保護のシステムの一つとして、賦課金制度がある。これは、ＤＡＴ(Digital Audio Taperecorder)、ＭＤで実施されているもので、ディジタル録音機器の利用者が製品価格に上乗せされた補償金を支払うものである。ネットワークが発展している今日では、ネットワークを介して配信されたコンテンツをパソコン（パーソナルコンピュータ）により受信し、再生することが行われるように、ハードウエア（プレーヤ、メディア）とコンテンツが１対１に対応しないことが多く、かかる賦課金制度は、著作権の保護のシステムとして、適しているとは言えない。

【０００５】

また、メディア例えばＣＤに複数の曲が記録されている場合に、ユーザは、その内の特定の１または数曲のみを聞きたい場合があり、メディア全体を購入したくはない場合もある。さらに、コピー防止技術のために、音楽コンテンツの宣伝・流通が阻害されることになる。むしろ、無料で音楽コンテンツを配信する方がその音楽コンテンツの宣伝・流通を短時間に行うことが可能となり、宣伝・流通のための費用を削減することも可能となる。

【０００６】

【発明が解決しようとする課題】

このような問題を考慮すると、配信が無料で、再生時に課金がなされる配信システムが好ましい。そのようなシステムにおいて、再生課金処理としては、種々のものがありうる。多種多様な再生課金に応じて、課金処理をすることは、従来では、なされていなかった。また、聴取権を生じさせるための聴取権データをユーザに安全に渡すことができる必要がある。

【０００７】

したがって、この発明の目的は、このような点に鑑み、ディジタルデータに付随する再生条件に従って課金処理を行うことが可能で、また、視聴権データを安

全に渡すことができ、さらに、再生条件に従ってディジタルデータを再生することが可能なデータ復号装置および方法、課金情報処理装置および方法、並びにデータ再生装置および方法を提供することにある。

【０００８】

【課題を解決するための手段】

上述した課題を解決するために、請求項１の発明は、符号化または暗号化されたディジタルデータを復号する復号装置において、

符号化または暗号化されたディジタルデータを復号する復号手段と、

視聴権データを記憶するための記憶手段と、

符号化または暗号化されたデータを復号する際に、ディジタルデータに付随されている再生条件情報の指示に従って記憶手段内の視聴権データに変更を加えることにより課金処理を行う課金制御手段とを備えたことを特徴とするデータ復号装置である。

【０００９】

請求項９の発明は、符号化または暗号化されたディジタルデータを復号する復号方法において、

符号化または暗号化されたディジタルデータを復号するステップと、

符号化または暗号化されたデータを復号する際に、ディジタルデータに付随されている再生条件情報の指示に従って記憶されている視聴権データに変更を加えることにより課金処理を行うステップとを備えたことを特徴とするデータ復号方法である。

【００１０】

請求項１０の発明は、決裁センターとデータ復号装置との間で、視聴権データを中継するための課金情報処理装置において、

複数のデータ復号装置の間で共用可能なように、可搬型とされたことを特徴とする課金情報処理装置である。

【００１１】

請求項１１の発明は、決裁センターとデータ復号装置との間で、視聴権データを中継するための課金情報処理装置において、

有線または無線通信手段を介して決裁センターに直接または他の機器を中継して接続できる通信手段と、

決裁センターから安全に視聴権データを得るための手段と、

視聴権データを記憶する記憶手段と、

外部の機器との間で安全に視聴権データの一部または全部を転送するための手段を有するインターフェースとからなることを特徴とする課金情報処理装置である。

【００１２】

請求項１７の発明は、決裁センターとデータ復号装置との間で、視聴権データを中継するための課金情報処理装置において、

外部の機器との間で安全に視聴権データの一部または全部を転送するための手段を有するインターフェースと、

視聴権データを記憶する記憶手段とを備え、

インターフェースは、ＩＣカードとの間で視聴権データの転送が可能なことを特徴とする課金情報処理装置である。

【００１３】

請求項２１の発明は、決裁センターとデータ復号装置との間で、視聴権データを中継するための課金情報処理方法において、

有線または無線通信手段を介して決裁センターに直接または他の機器を中継して接続するステップと、

決裁センターから安全に視聴権データを得るステップと、

視聴権データを記憶するステップと、

外部の機器との間で安全に視聴権データの一部または全部を転送するステップとからなることを特徴とする課金情報処理方法である。

【００１４】

請求項２２の発明は、圧縮符号化および／または暗号化されたディジタルデータを再生するデータ再生装置において、

ディジタルデータを復号する復号装置を備え、

復号装置は、

符号化または暗号化されたディジタルデータを復号する復号手段と、

視聴権データを記憶するための記憶手段と、

符号化または暗号化されたデータを復号する際に、ディジタルデータに付随されている再生条件情報の指示に従って記憶手段内の視聴権データに変更を加えることにより課金処理を行う課金制御手段とを備えたことを特徴とするデータ再生装置である。

【００１５】

請求項２３の発明は、圧縮符号化および／または暗号化されたディジタルデータを再生するデータ再生方法において、

符号化または暗号化されたディジタルデータを復号するステップと、

符号化または暗号化されたデータを復号する際に、ディジタルデータに付随されている再生条件情報の指示に従って記憶されている視聴権データに変更を加えることにより課金処理を行うステップとを備えたことを特徴とするデータ再生方法である。

【００１６】

再生条件情報に従って視聴権データに変更を加えることによって、多種多様な課金処理に対応することができる。また、視聴権データをユーザに渡すことが安全に行われる。

【００１７】

【発明の実施の形態】

以下、この発明の一実施形態について説明する。最初に図１を参照してコンテンツ流通システムの概略について説明する。図１において、１０１がコンテンツ供給事業者を示し、１０２がコンテンツサーバを示す。コンテンツ供給事業者１０１がコンテンツの制作およびその配給を行う。レコード会社は、コンテンツ供給事業者１０１の一つである。また、コンテンツに関しての圧縮符号化、暗号化、ウォーターマークの埋め込みもコンテンツ供給事業者１０１が行う。コンテンツサーバ１０２には、コンテンツ供給事業者１０１が制作したコンテンツが蓄積される。

【００１８】

１０３は、著作権管理機構を示す。例えばＪＡＳＲＡＣ（日本音楽著作権協会）は、著作権管理機構１０２の具体例である。コンテンツ供給事業者１００は、著作権管理機構１０３に対して権利登録を行い、著作権管理機構１０３から著作権料を受け取る。

【００１９】

１０４がコンテンツの再生機能を有するユーザ機器を示す。ユーザ機器１０４は、配信されたコンテンツを再生する。すなわち、暗号化を復号し、また、圧縮符号化を復号することによって、コンテンツを再生することができる。コンテンツサーバ１０２とユーザ機器１０４との間には、必要に応じてコンテンツ配信事業者が介在し、ユーザに対してコンテンツサーバ１０２内のコンテンツを配信する。配信事業者が使用する配信手段としては、幾つかのものがある。その一つは、販売店１０５である。例えば雑誌の付録として、コンテンツが記録されたメディアが配付される。また、インターネット、ＣＡＴＶ(cable television)のような有線ネットワーク１０６がコンテンツの配信手段として使用される。さらに、携帯電話網１０７、衛星放送、衛星通信等の衛星ネットワーク１０８もコンテンツの配信手段として使用される。

【００２０】

この発明では、上述したコンテンツ配信手段として、有料で配信されるコンテンツの配信手段を利用することを妨げるものではない。媒体例えばＣＤの場合には、記録されている楽曲に対しての著作権料がＣＤの価格に含まれている。配付を無料とし、復号（再生）に課金されるコンテンツをＣＤ上の有料コンテンツが記録された領域とは別の領域に記録するようにしても良い。

【００２１】

図１中では、販売店１０５が配付する媒体の一つとしての拡張ＣＤ１２１が示されている。拡張ＣＤ１２１の内周側の領域１２２は、既存のＣＤと同一のフォーマットで、配付が有料で、再生が無料とされた楽曲データが記録された領域である。また、外周側の領域１２３は、この発明が適用されたコンテンツ、すなわち、配付が無料で、再生が有料のコンテンツが記録された領域である。コンテン

ツは、圧縮符号化されているので、領域１２３が少なくても必要な長さの音楽データを記録することができる。

【００２２】

ＣＤ以外にＭＤ、メモリカード等の媒体の場合にも、互いに区別できる領域として、配付が有料で、且つ再生が無料のコンテンツと、配付が無料で、且つ再生が有料のコンテンツとを記録することができる。また、衛星テレビジョン放送を利用して音楽コンテンツを配信するサービスを利用して配付が無料で、再生が有料のコンテンツを配信しても良い。

【００２３】

ユーザ機器１０４は、コンテンツを無料で受け取ることができる。また、受け取ったコンテンツの再配付も自由に行うことができる。ここで、無料というのは、通信費、電気代等の実費を含まず、著作権料に関して無料という意味である。ユーザ機器１０４が受け取ったコンテンツを再生、より具体的には、暗号化を復号する時に課金処理がなされる。課金処理のために、プリペイドデータ１０９が使用される。プリペイドデータ１０９は、プリペイドカード、セキュアデコーダ内のメモリに格納されている。プリペイドデータ１０９は、プリペイドデータ管理会社の管理下で、課金チャージャによって書き換えることが可能とされている。プリペイドデータ１０９は、例えば再生可能な度数であり、ユーザ機器１０４が課金の対象のコンテンツを再生する度に、度数が減算される。

【００２４】

また、コンテンツ供給事業者１０１、著作権管理機構１０３、ユーザ機器１０４と関係して代金決裁のために、課金／決裁センター１１０が存在している。課金／決裁センター１１０は、認証／課金サーバ１１１を備えている。課金／決裁センター１１０は、銀行、クレジット会社等である。

【００２５】

ユーザ機器１０４が受け取ったコンテンツの再生を要求すると、認証／課金サーバ１１１に対してユーザ機器１０４の認証を要求する（Ａ１の経路で示す）。ユーザ機器１０４が正規のものであり、認証が成立すると、認証／課金サーバ１１１は、ユーザ機器１０４に対して課金の要求を行う（経路Ａ２）。また、ユー

ザ機器１０４は、課金／決裁センター１１０との間で、代金決裁を行う（経路Ａ３）。

【００２６】

課金／決裁センター１１０は、認証／課金サーバ１１１に対して、経路Ａ４で示すように、課金がされたことを伝達すると共に、コンテンツサーバ１０２に対してコンテンツを要求する（経路Ａ５）。コンテンツサーバ１０２が認証／課金サーバ１１１に暗号化を復号するための鍵データを渡す（経路Ａ６）。認証／課金サーバ１１１がユーザ機器１０４に対して、鍵データを渡す（経路Ａ７）。ユーザ機器１０４は、この鍵データによって、暗号を復号化し、再生することができる。復号化がされることをもって、そのコンテンツの再生がされたものと判断され、プリペイドデータ１０９の度数が例えば－１される。度数が０に達すると、ユーザ機器１０９が復号化ができなくなる。

【００２７】

図２は、プリペイドデータ１０９の管理システムの一例を示す。ユーザ１０４に対応するものとして、プレーヤ２０１が示されている。プレーヤ２０１は、セキュアデコーダ２０２を内蔵している。また、プレーヤ２０１は、例えば携帯形オーディオ機器である。図２において、破線で示すように、プレーヤ２０１が再生する媒体（光ディスク、メモリカード等）には、音楽コンテンツが記録されている。音楽コンテンツの配信の方法は、図１に示したように、種々のものが使用できる。

【００２８】

２０４は、プリペイドデータチャージャを示す。プリペイドデータチャージャ２０４は、プレーヤ２０１のセキュアデコーダ２０２とプリペイドデータ管理会社２０５またはデータ販売機２０６との間に存在してプリペイドデータ中継器として機能する。セキュアデコーダ２０２とプリペイドデータチャージャ２０４とが通信を行い、プリペイドデータがプリペイドデータチャージャ２０４からセキュアデコーダ２０２内のメモリに対して転送される。プリペイドデータは、例えばプレーヤ２０１の再生可能回数情報または再生可能時間に対応している。また、プレーヤ２０１からプリペイドデータチャージャ２０４に対して、プレーヤ２

０１の再生履歴情報（再生ログ）が伝送される。再生ログは、復号したディジタルデータの識別子および／または復号の条件を含む。具体的には、聴取した音楽コンテンツの種類、再生回数、再生時間等の情報を含んでいる。セキュアデコーダ２０２とプリペイドデータチャージャ２０４とは、認証を行い、認証が成立すると、暗号化されたプリペイドデータおよび再生ログの伝送がなされる。

【００２９】

プリペイドデータは、プリペイドデータ管理会社２０５またはプリペイドデータ販売機２０６からプリペイドデータチャージャ２０４に渡される。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。プリペイドデータチャージャ２０４に吸い上げられた再生ログは、プリペイドデータ管理会社２０５またはプリペイドデータ販売機２０６に渡される。プリペイドデータ販売機２０６は、プリペイドデータ管理会社２０５からプリペイドデータを受け取ると共に、再生ログをプリペイドデータ管理会社２０５へ送る。さらに、入手するプリペイドデータの代金を管理会社２０５に支払う。

【００３０】

プリペイドデータ管理会社２０５とプリペイドデータチャージャ２０４との間では、例えば電話回線２０７を介してプリペイドデータおよび再生ログの送受信がなされる。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。プリペイドデータの決裁に関して、銀行、クレジット会社等の課金／決裁センター２０８が存在している。課金／決裁センター２０８は、予め登録してあるユーザの銀行口座からプリペイドデータ管理会社２０５の依頼に基づいて、セキュアデコーダ２０２に書き込んだプリペイドデータ相当する金額を引き落とす。

【００３１】

さらに、プリペイドデータ管理会社２０５は、コンテンツ供給事業者１０１からプリペイドデータに関するサービスの管理の委託を受ける。また、プリペイドデータ管理会社２０５は、コンテンツ供給事業者１０１に対してプリペイドデータに関する技術の提供を行い、さらに、楽曲聴取料を支払う。コンテンツ供給事業者１０１は、図１を参照して説明したように、著作権管理機構１０３に対して

著作権の登録を行うことによって、著作権の管理を依頼し、著作権管理機構１０３から著作権料を受け取る。

【００３２】

図２では省略しているが、プリペイドデータチャージャ２０４は、他のチャージャとの間で、通信装置例えば非接触通信装置を通じて、視聴権データの一部または全部を移動・合算・分割可能とされている。また、プリペイドデータチャージャ２０４は、プレーヤ２０１のセキュアデコーダ２０２以外にＩＣカードの構成のプリペイドカードに対して聴取権データを転送可能とされている。

【００３３】

図３は、セキュアデコーダ２０２を有するプレーヤ２０１の全体的構成を示す。セキュアデコーダ２０１は、破線で示すように、１チップのＩＣとして構成されたものである。また、セキュアデコーダ２０１は、所謂タンパーレジスタント(tamper resistant)の構成とされている。すなわち、外部からは、その内容が分からないような構成とされ、改ざんができない構成とされている。

【００３４】

媒体１には、圧縮符号化され、また、暗号化された音楽データが記録されている。さらに、再生課金処理に必要なデータが圧縮符号化、暗号化されたデータに付随している。圧縮符号化、暗号化されたデータをコンテンツデータと称し、再生課金処理のためのデータを付随データと称する。但し、この発明では、圧縮符号化と暗号化との両方が施されていることは、必ずしも必要ではない。圧縮符号化のみでも、その復号方法が非公開であれば、著作権保護の目的を果たすことが可能である。

【００３５】

媒体１としては、メモリカード、記録可能な光ディスク、読み出し専用の光ディスク等を使用できる。記録可能な媒体の場合では、上述したように、衛星ネットワーク、携帯電話ネットワーク、インターネット等のネットワークを介して配信されたデータをダウンロードすることができる。媒体１に記録されているコンテンツデータおよび付随データがインターフェース２を介してセキュアデコーダ２０２に供給される。セキュアデコーダ２０２からは、アナログオーディオ信号

が出力される。アナログオーディオ信号は、アンプ等を介してスピーカ、ヘッドフォン等によって再生される。

【００３６】

セキュアデコーダ２０２は、暗号化の復号器１１と、圧縮符号化の伸長器１２と、Ｄ／Ａ変換器１３とを有している。暗号化としては、ＤＥＳ(Data Encryption Standard)を使用できる。ＤＥＳは、平文をブロック化し、ブロック毎に暗号変換を行うブロック暗号の一つである。ＤＥＳは、６４ビットの入力に対して６４ビット（５６ビットの鍵と８ビットのパリティ）のキーを用いて暗号変換を行い、６４ビットを出力する。ＤＥＳ以外の暗号化を使用しても良い。例えばＤＥＳは、暗号化と復号化に同一の鍵データを使う共通鍵方式であるが、暗号化と復号化に異なる鍵データを使う公開鍵暗号の一例であるＲＳＡ暗号を採用しても良い。鍵データは、上述したように、認証が成立したユーザ機器１０４に対して渡される。

【００３７】

セキュアデコーダ２０２には、ＣＰＵを含む制御部１４と、制御部１４と外部のＣＰＵとの通信を行うためのＣＰＵインターフェース１５と、メモリ部１６と、プリペイドデータをプリペイドチャージャから受信し、再生ログをプリペイドチャージャに伝送するための通信部１７およびアンテナ１８とが設けられている。制御部１４は、復号器１１における復号の前段で分離された付随データを受け取り、復号化、伸長化を行うための制御を行う。

【００３８】

また、通信部１７およびアンテナ１８は、非接触でプリペイドデータチャージャとの間で通信を行うためのものである。この通信は、認証がされることを条件として、暗号化されたプロトコルを使用してなされる。データのみならず、電力をチャージャから受信可能とされているので、プレーヤ２０１全体の電源がオフであっても、プリペイドデータの受信と、再生ログの送信とを行うことができる。受け取ったプリペイドデータは、メモリ部１６に格納される。さらに、プレーヤ２０１の再生ログもメモリ部１６に記憶される。メモリ部１６は、電源オフとされても、その記憶内容が保持される不揮発性メモリである。

【００３９】

なお、コピー出力が復号器１１からセキュアデコーダ２０２の外部に出力することが可能とされている。出力するか否かは、制御部１４により制御される。出力されるコピー出力は、付随情報とコンテンツデータである。さらに、復号器１１および伸長器１２は、制御部１４の指示に基づいて、復号処理および伸長処理をそれぞれ省略する機能を有している。それによって、暗号化されていないオーディオデータ、並びに圧縮符号化されていないオーディオデータ（リニアＰＣＭ）を再生することが可能とされている。

【００４０】

プレーヤ２０１の全体の動作を制御するために、２１で示すシステムコントローラが備えられている。システムコントローラ２１は、ＣＰＵで構成され、セキュアデコーダ２０２内の制御部１４と通信を行うことによって、セキュアデコーダ２０２の動作を制御する。また，システムコントローラ２１とバスを介して操作部２２、ディスプレイ２３、メモリ部２４、モデム２５が接続されている。さらに、システムコントローラ２１が媒体１の再生動作、並びに媒体インターフェース２の動作を制御する。

【００４１】

操作部２２は、ユーザが操作するスイッチ、キー等であり、プレーヤ２０１の動作を制御する指示を発生する。ディスプレイ２３は、例えば液晶からなるもので、プレーヤ２０１の動作を制御するためのメニューを表示したり、動作状態を表示するために使用される。メモリ部２４は、システムコントローラ２１内のメモリの容量が少ないために設けられた外部メモリである。モデム２５は、公衆回線と接続され、外部とのデータの通信に使用される。例えば、セキュアデコーダ２０２のメモリ部１６内の再生ログをメモリ部２４に転送することによって、残りの再生可能回数または再生可能時間をディスプレイ２３に表示したり、再生ログをモデム２５を介して送信することが可能とされている。さらに、プリペイドデータをモデム２５を介して受信することも可能である。

【００４２】

ユーザが操作部２２を操作することによって、媒体１内の所望のコンテンツの

再生を指示する。そのコンテンツが再生に関して無料のものであれば、セキュアデコーダ２０２を通ってアナログ出力が発生しても、メモリ部１６に格納されているプリペイドデータが変更されない。若し、再生したコンテンツが再生課金の対象である場合には、メモリ部１６内のプリペイドデータが変更される。

【００４３】

課金処理としては、種々のタイプが可能である。課金処理としては、大きく分けて、買取型と、グロスに視聴料金をとるタイプと、セキュアデコーダで暗号の復号化を行うごとに視聴料金を課する度数タイプとがある。買取型は、一旦買い取った後では、再生処理に対して課金されないタイプである。グロスに視聴料金をとるタイプは、視聴料金をまとめて支払う月極めタイプ、視聴期間、視聴時間を限定するタイプ等である。

【００４４】

セキュアデコーダで暗号の復号化を行うごとに視聴料金を課す度数タイプとして、幾つかの形態が可能である。第１の形態は、予め設定された金額（プリペイドカード、電子マネー）または度数からコンテンツの再生処理の度に、金額または度数を減算するものである。残高または残り度数が不足する場合には、再生ができなくなる。第２の形態は、コンテンツの再生処理の度に、金額または度数が加算されるものである。予め設定した金額または度数に累積金額または累積度数が達すると、再生ができなくなる。第３の形態は、コンテンツの再生時間に応じて、度数または金額が加算または減算されるものである。

【００４５】

金額または度数は、一定のものであっても良く、また、コンテンツに応じて重み付けされたものでも良い。また、課金処理は、コンテンツの１タイトル（音楽の例では、１曲）またはコンテンツの複数タイトル（音楽の例では、アルバム）と対応して行われる。

【００４６】

また、コンテンツの再生処理の定義の方法としては、コンテンツ全体を再生した場合に、再生を行ったものとしても良いし、また、コンテンツの再生時間が所定時間以上の場合を再生を行ったものとしても良い。さらに、普及・流通を促進

するためのプロモーション用のコンテンツの再生に対しては課金されない。また、課金の対象となるコンテンツであっても、例えばコンテンツの先頭部分例えば先頭から１０秒間の再生を無料としたり、コンテンツのハイライト部分のみの再生を無料としても良い。このように、再生処理に対して課金されるコンテンツと、再生処理が無料のコンテンツとが混在する場合に、付随情報によって課金／無料が識別される。

【００４７】

付随情報は、コンテンツデータ（圧縮符号化および暗号化されたコンテンツ例えばオーディオデータ）の前に付加されたデータである。付随情報は、必要に応じて暗号化される。また、記録可能な媒体には、コンテンツデータの前に付加されて記録されるか、または媒体１のデータ管理用領域に記録される。読み出し専用の媒体の場合には、データ管理領域に付随情報が記録される。光ディスクの場合では、一般的にディスクの最内周側の領域に管理領域が設けられる。メモリカードの場合には、例えば音楽データの１曲を１ファイルとして扱うようにしたファイル管理データが規定される。

【００４８】

付随データには、課金されるコンテンツか、無料のコンテンツかを指示する課金識別子、並びに上述したような買取型、グロス型、度数型等の課金タイプを区別し、各課金タイプにおける課金条件を指示する再生条件ラベルが含まれる。一例として、買取型の場合では、買取価格のデータが再生条件ラベルに記述され、グロス型の再生回数を制限する場合では、再生回数のデータが再生条件ラベルに記述され、グロス型の再生期間を制限する場合では、再生期間のデータ（１日、１週間、１ヵ月等）が再生条件ラベルとして記述され、度数型の場合では、度数のデータ（１円／２分、１円／１分、１円／３０秒、・・・）が再生条件ラベルとして記述される。さらに、課金を前提としているコンテンツであっても、無料で視聴できる場合の条件を再生条件ラベルに記述することもできる。

【００４９】

また、付随情報中に、コンテンツデータの圧縮符号化の種類を示すための情報、暗号の種類および暗号のパラメータを示すための情報、チャンネル数の情報、

ビットレートの情報等を記録しても良い。

【００５０】

さらに、付随情報中には、ＣＤ、ＭＤ、記録可能な光ディスク、不揮発性メモリを含むメモリカード等の媒体を一意に識別可能とするためのメディアＩＤ例えばシリアル番号が含まれる。さらに、付随情報中には、デコーダＩＤが配置される。デコーダＩＤは、ユーザの端末、ユーザのプレーヤ等に内蔵されているセキュアデコーダを一意に識別可能とするためのＩＤ例えばシリアル番号である。

【００５１】

次に、図４のフローチャートを参照してプレーヤ２０１（図３参照）においてなされる課金処理の一例について説明する。この処理は、セキュアデコーダ２０２内の制御部１４およびシステムコントローラ２１によってなされるものである。最初のステップＳ１は、媒体１に再生しようとするコンテンツが存在しているような再生スタンバイ状態である。具体的には、ＥＭＤにより配信されたコンテンツが媒体１に格納されている場合、媒体１に既にコンテンツが記録されている場合等が再生スタンバイに該当する。ステップＳ２では、ユーザが操作部２２の再生ボタンを押すことによって再生指示がされたかどうかが決定される。

【００５２】

ステップＳ２の結果が否定であることは、コピーの操作を意味するものとされている。ステップＳ３において、無料再生用コンテンツのコピーか否かが決定される。無料再生用コンテンツとは、再生が課金されないコンテンツを意味する。付随情報中に含まれる識別子を参照してステップＳ３の決定がなされる。無料再生用コンテンツであれば、著作権保護のために、セキュアデコーダ２０２からの暗号が復号化されたコピー出力が禁止される（ステップＳ４）。

【００５３】

若し、無料再生用コンテンツのコピーでない、すなわち、課金再生用コンテンツのコピーであるとステップＳ３で決定されると、課金再生用コンテンツのコピーがセキュアデコーダ２０２から出力される（ステップＳ５）。課金再生用コンテンツのコピーは、自由になされる。但し、このコピー出力は、付随情報と暗号化、圧縮符号化がされたデータである。

【００５４】

ステップＳ２において、再生動作が指示されたものと決定されると、ステップＳ６において、課金処理を受け入れるか否かが問われる。例えばプレーヤ２０１のディスプレイ２３にメッセージが表示され、ユーザが操作部２２の操作によって回答するようになされる。ユーザが課金処理を受け入れない場合には、無料再生ができない（ステップＳ７）。但し、再生条件ラベルによって指示される部分的無料再生例えば曲の先頭部分またはハイライト部分の再生を無料で行うことが許される場合もある。課金処理を受け入れる場合には、ステップＳ８において、ディスプレイ２３上に、現に再生しようとするコンテンツに関する再生課金条件が提示される。付随情報中の再生条件ラベルの情報に基づいて課金条件の提示がなされる。

【００５５】

ステップＳ９では、課金タイプが買取型かどうかが決定される。買取型であれば、買取用の課金がなされる（ステップＳ１０）。そして、ステップＳ１１において、セキュアデコーダ２０２の復号器１１では、鍵を使用して暗号を復号化し、ステップＳ１２において、無料再生を行う。この場合、無料再生するコンテンツのコピーが禁止される。但し、ムーブ、すなわち、コピーと異なり元のデータが残らない処理は、可能である。

【００５６】

ステップＳ９において、買取型でないと決定されると、ステップＳ１３においてグロス型例えば月極型かどうかが決定される。月極契約が存在しているときには、ステップＳ１４において、契約された楽曲か否かが決定される。そうであれば、ステップＳ１５において、無料再生がなされる。課金再生用コンテンツのコピーは自由に行うことができる。

【００５７】

ステップＳ１３において、月極型でないと決定されると、そのコンテンツは、度数型で課金されるものと決定される。そして、ステップＳ１７において、暗号の復号化がなされ、ステップＳ１８において、課金再生がなされる。課金再生では、上述したように、再生の度数、再生時間等に応じて課金される。また、課金

再生用コンテンツのコピーは、自由にできる。さらに、ステップＳ１４において、月極契約の範囲内でないと決定された場合も、課金再生の処理（ステップＳ１７、ステップＳ１８）がなされる。

【００５８】

図５は、プリペイドデータチャージャ２０４の一例の構成を示す。チャージャ２０４は、例えば持ち運び可能な可搬型の構成とされている。３０１がチャージャ全体を制御するＣＰＵを示し、３０２が暗号化・復号化モジュールを示し、３０３がディスプレイ（例えば液晶ディスプレイ）を示し、３０４がユーザによって操作されるキー・ボタンを示す。ディスプレイ３０３には、チャージャの動作に関連するメニュー、課金処理条件等が表示される。暗号化・復号化モジュール３０２は、送信時の暗号化の処理と、受信時の暗号の復号化の処理とを行う。３０５は、データチャージャ個別ＩＤを示す。データチャージャ個別ＩＤ３０５は、例えば再生ログと共に決裁センターへ送信され、データチャージャと再生ログの対応関係が分かるようになされる。

【００５９】

また、決裁センター（図２中のプリペイドデータ管理会社２０５）との通信のために、モデム３０６およびＵＳＢ(Universal Serial Bus)通信モジュール３０７が設けられている。モデム３０６によって、電話回線を介して決裁センターとの通信が行われ、決裁センターからプリペイドデータを受け取り、また、決裁センターに対して再生ログを送信することができる。ＵＳＢ通信モジュール３０７を使用し、パーソナルコンピュータおよびインターネットによって同様に決裁センターとの通信が可能である。

【００６０】

決裁センターからデータチャージャ２０４が受信したプリペイドデータがプリペイドデータメモリ３０８に格納される。また、プレーヤ２０１のセキュアデコーダ２０２から受け取った再生ログが使用状況メモリ３０９に格納される。必要に応じてチャージャ２０４のログが再生ログに付加されたログデータが決裁センターへ送信される。メモリ３０８および３０９は、電源オフとされても、その記憶内容が保持される不揮発性メモリである。

【００６１】

また、非接触通信モジュール３１０およびアンテナ３１１は、非接触でプレーヤ２０１との間で通信を行うためのものである。この通信は、認証がされることを条件として、暗号化されたプロトコルを使用してなされる。データのみならず、セキュアデコーダ２０２が動作するのに必要な電力をプレーヤに送信可能とされている。したがって、プレーヤ２０２のメインの電源がオフであっても、プリペイドデータおよび再生ログの授受が可能とされている。アンテナ３１１以外にライン接続用の端子も備えられている。なお、非接触通信モジュール３１０およびアンテナ３１１またはラインを使用してプリペイドデータ販売機２０６との通信を行うようになされる。

【００６２】

図６は、セキュアデコーダ２０２のより詳細な構成、すなわち、課金処理に関する機能的構成を示す。図３に示される構成要素と対応する部分には、同一符号を付して示す。媒体１からの暗号化され、且つ圧縮符号化されたコンテンツデータと付随データとからなる再生データが復号器１１に供給される。復号器１１には、媒体１を一意に識別可能とするためのメディア個別ＩＤも供給される。復号器１１によって暗号の復号がなされる。

【００６３】

復号器１１の出力データが再生条件ラベル検出部４０１に供給され、付随データ中の再生条件ラベルが検出される。検出された再生条件ラベルがセキュアデコーダ２０２の処理に使用される。伸長器１２では、圧縮符号化の復号がなされる。伸長器１２の出力データがウォーターマーク検出部４０２に供給される。ウォーターマーク検出部４０２は、アナログ出力時に付加したウォーターマークを検出し、検出されたウォーターマークと再生条件ラベルとに基づいて、再生条件ラベルが改ざんされたか否かをチェックする。

【００６４】

４０３は、聴取権カウンタを示す。聴取権カウンタ４０３においては、後でより詳細に説明するが、再生データを復号する度に、聴取権データに対して変更を加える。例えばメモリ部１６に格納されているプリペイドデータ例えば度数デー

タを減算する処理を行う。メモリ部１６に格納されるプリペイドデータは、アンテナ１８（またはライン）と通信モジュール１７とによって、上述したプリペイドデータチャージャ２０４から送信されたものである。通信モジュール１７内には、暗号化・復号化のモジュールが設けられている。なお、ここでは、楽曲データを取り扱うために、聴取権の用語を使用しいてるが、映像データを含めて考えた時には、聴取権の代わりに視聴権の用語が使用される。

【００６５】

聴取権カウンタ４０４において、聴取権に関する処理がされると、ウォーターマーク付加部４０４において、出力されるデータに対してウォーターマークが付加される。ウォーターマークは、楽曲データに存在する冗長な部分例えば出力されるオーディオデータの下位のビットを利用することでウォーターマークを付加できる。付加されたウォーターマークは、アナログ信号に変換しても残り、且つウォーターマークを除去することが不可能か、非常に困難なものである。付加されるウォーターマークは、再生条件ラベルの全体または一部のデータと、デコーダ個別ＩＤ４０５の情報を含むものである。ウォーターマークが付加されたデータがＤ／Ａ変換器１３によってアナログ出力に変換され、セキュアデコーダ２０２の外部へ出力される。上述したウォーターマーク検出部４０２は、このように付加されたウォーターマークを検出するものである。

【００６６】

セキュアデコーダ２０２がＩＣカードのインターフェースを持ち、また、プリペイドデータチャージャ２０４が決裁センターまたは金融会社から電子マネーを受け取り、受け取った電子マネーをセキュアデコーダ２０２が備えているインターフェースを介してＩＣカードに記録するようにしても良い。すなわち、プリペイドデータの書き込みに対して、オプショナルなものとして電子マネーの記録装置としての機能を持たせることができる。

【００６７】

図７は、聴取権カウンタ４０３の部分をより詳細に示す。ここでは、課金処理が度数型で行われる場合に適用される例について説明する。すなわち、予め設定された度数から楽曲データの再生処理の度に、度数を減算したり、楽曲データの

再生処理の度に、度数が加算されたり、楽曲データの再生時間に応じて、度数が加算または減算される。

【００６８】

再生データ例えば楽曲データから再生条件ラベル抜き出し部４１１が再生条件ラベルを抜き出す。再生条件ラベルには、課金条件が含まれている。また、基本クロック抜き出し部４１２によって、楽曲データから課金の基本クロックが抜き出される。基本クロックは、楽曲データが伸長器１２から出力されている期間のみ発生する。基本クロックの周期は、楽曲データごとには固定であり、２分、１分、３０秒等の周期で発生する。基本クロックの複数個をこれらの周期に対応させても良い。そして、周期が課金の単位として扱われる。すなわち、１周期が一つの度数に対応され、また、時間の単位に対応される。

【００６９】

抜き出された基本クロックと再生条件ラベルに基づいて、プリペイドデータのカウント制御部４１３がカウントを制御する。すなわち、再生条件ラベルを参照して、プリペイドデータのメモリ４１４（メモリ部１６の一部）に格納されているプリペイドデータに対して減算または加算処理を行い、プリペイドデータを書き換える。また、再生時間または再生期間を再生条件としている場合には、タイマー／カレンダーに対して、再生時間の累積処理または現在日時と再生可能期限との照合処理がなされる。

【００７０】

プリペイドデータカウント制御部４１３は、さらに、再生可能かどうかを判断する。例えば再生した度数を減算して、残りが０となると、再生不可能と判断する。また、累積度数が設定された度数に到達したり、再生時間の累積が設定された時間に到達したり、現在の日時が再生期限を越えたりすると、同様に、再生不可能と判断する。判断結果に基づいて、楽曲データのゲート部４１６が制御される。再生可能な場合には、楽曲データがゲート部４１６を通過して出力され、一方、再生不可能な場合には、楽曲データの出力がゲート部４１６によって禁止される。

【００７１】

図６に示すセキュアデコーダ２０２におけるウォーターマーク検出部４０２の処理について、図８のフローチャートを参照して説明する。ウォーターマークの検出処理Ｓ２１が開始されると、ステップＳ２２において、ウォーターマークの抜き出し処理がなされる。そして、ステップＳ２３では、ウォーターマークが正しく抜き出せたか否かが決定される。

【００７２】

ウォーターマークが正しく抜き出せないと決定されると、ウォーターマークが付加されていないものとして、楽曲再生データを出力する（ステップＳ２４）。ウォーターマークが正しく抜き出せたときには、ステップＳ２５において、ウォーターマークに再生条件ラベルのデータが入っているか否かが決定される。再生条件ラベルが入っていないと決定されると、楽曲再生データを出力する（ステップＳ２４）。

【００７３】

ステップＳ２５において、ウォーターマークに再生条件ラベルのデータが入っているものと決定されると、ステップＳ２６において、ウォーターマーク中の再生条件ラベルと、再生条件ラベル検出部４０１において検出した付随情報中の再生条件ラベルとの照合処理がなされる。ステップＳ２７では、これらの再生条件ラベルが同一か否かが決定される。同一であるならば、楽曲再生データの出力（ステップＳ２４）がなされる。若し、同一でないときには、再生条件ラベルが改ざんされた可能性があると判断し、楽曲再生データを出力しない（ステップＳ２８）。

【００７４】

図９は、セキュアデコーダ２０２のウォーターマーク付加部４０４が行うウォーターマーク付加処理を示すフローチャートである。ウォーターマークの付加処理Ｓ３１が開始されると、ステップＳ３２において、ウォーターマーク検出部４０２がウォーターマークを正しく抜き出せたか否かが決定される。正しく抜き出せたならば、ウォーターマークを付加しないで再生データを出力する（ステップＳ３３）。すなわち、再生データに埋め込まれていたウォーターマークが変更さ

れない。

【００７５】

若し、ステップＳ３２の結果が否定であれば、ステップＳ３４およびＳ３５によってウォーターマークに入れるデータが生成される。ステップＳ３４は、再生条件ラベルからウォーターマークに入れるデータを生成する処理である。再生条件ラベルの一部または全てをウォーターマークとして入れる。ウォーターマークとして埋め込むデータは、再生条件ラベルのデータそのものに限らず、ハッシュ値等の演算処理されたものでも良い。また、ステップＳ３５は、セキュアデコーダの個別ＩＤからウォーターマークに入れるデータを生成する処理である。セキュアデコーダ個別ＩＤの一部または全部のデータがウォーターマークに入れられる。個別ＩＤを入れることによって、ウォーターマークを付加したセキュアデコーダを特定することができる。

【００７６】

そして、ステップＳ３６において、上述したように生成したデータからなるウォーターマークが楽曲データに対して埋め込まれる。上述したように、楽曲データの冗長な部分を利用してウォーターマークが埋め込まれる。ウォーターマークは、ディジタル的に付加されるが、アナログ信号に変換されても残り、また、ウォーターマークを除去することは、不可能か、非常に困難である。ステップＳ３７では、ウォーターマークを付加して再生データが出力される。

【００７７】

なお、上述した実施形態では、主としてオーディオコンテンツについて説明したが、オーディオ以外のビデオデータ、静止画像データ、文字データ、コンピュータグラフィックデータ、ゲームソフトウェア、およびコンピュータプログラム等のコンテンツに対しても、上述したのと同様にこの発明を適用することができる。

【００７８】

【発明の効果】

以上の説明から明らかなように、この発明によれば、種々の課金処理条件に対応して課金処理を行うことができる。また、この発明は、視聴権データを安全に

ユーザに対して渡すことができる。

【図面の簡単な説明】

【図１】

この発明の一実施形態のシステム全体の概略を示すブロック図である。

【図２】

この発明の一実施形態におけるプリペイドデータに関する説明のためのブロック図である。

【図３】

この発明の一実施形態におけるプレーヤの一例のブロック図である。

【図４】

この発明の一実施形態における課金処理の一例を説明するためのフローチャートである。

【図５】

この発明の一実施形態におけるプリペイドデータチャージャの一例のブロック図である。

【図６】

この発明の一実施形態におけるセキュアデコーダのより詳細なブロック図である。

【図７】

セキュアデコーダの課金処理に関連する部分の構成を示すブロック図である。

【図８】

セキュアデコーダにおけるウォーターマークの検出の処理を説明するためのフローチャートである。

【図９】

セキュアデコーダにおけるウォーターマークの付加の処理を説明するためのフローチャートである。

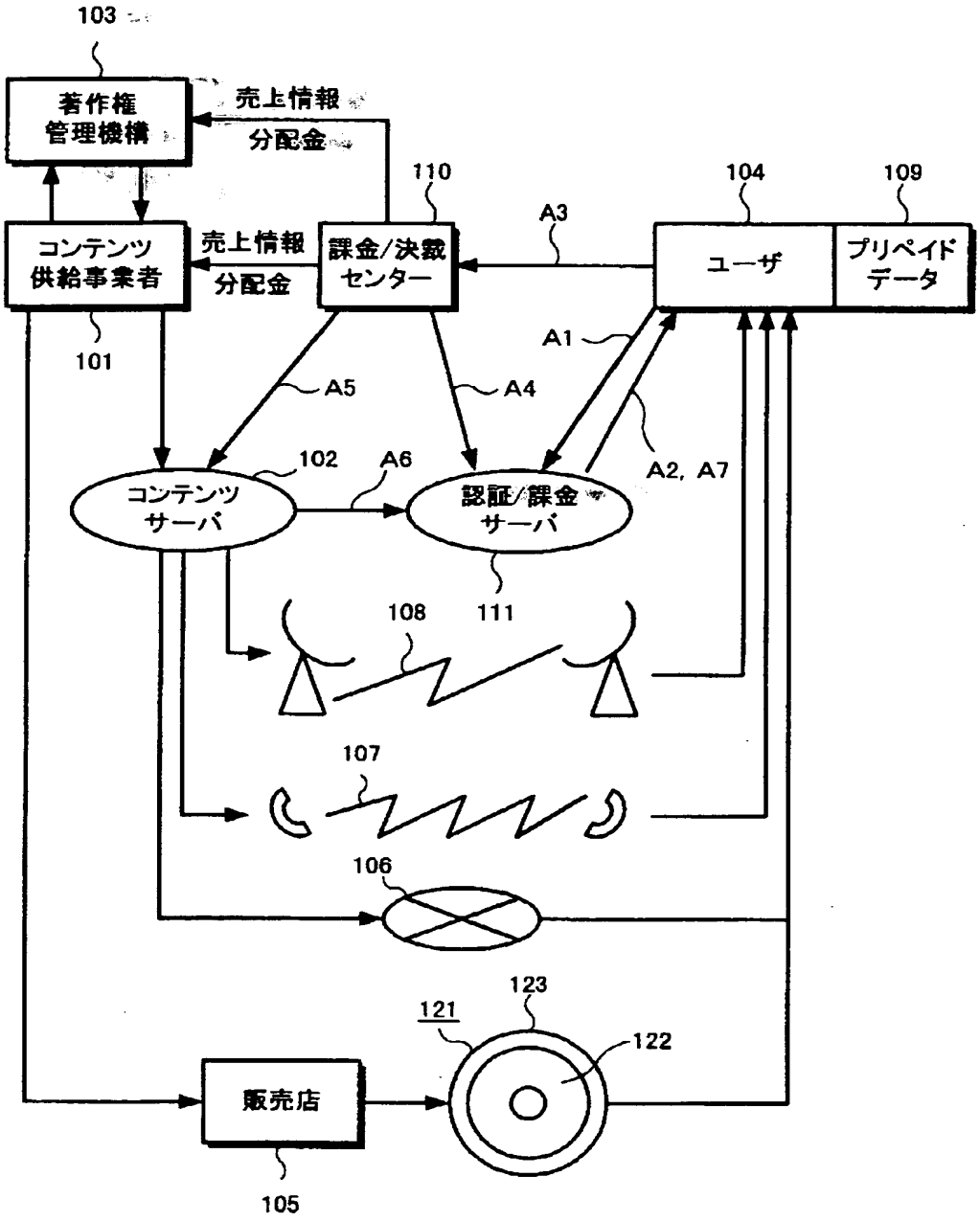
【符号の説明】

１・・・コンテンツの格納された媒体、１１・・・暗号化の復号器、１２・・・圧縮符号化の伸長器、２１・・・システムコントローラ、１０１・・・コンテン

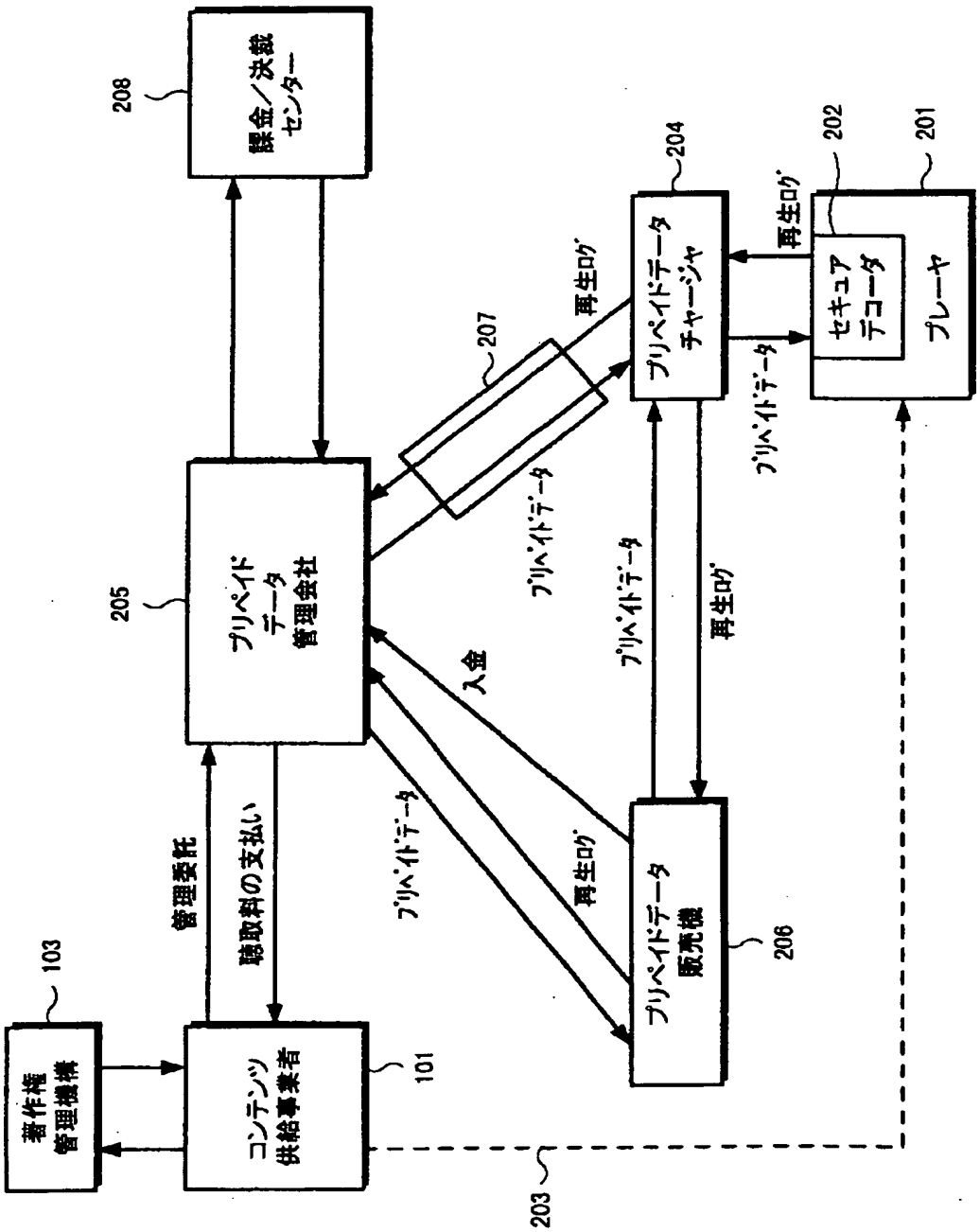
ツ供給事業者、１０３・・・著作権管理機構、１０４・・・ユーザ機器、１０９・・・プリペイドデータ、２０１・・・プレーヤ、２０２・・・セキュアデコーダ、２０４・・・プリペイドデータチャージャ

【書類名】　図面

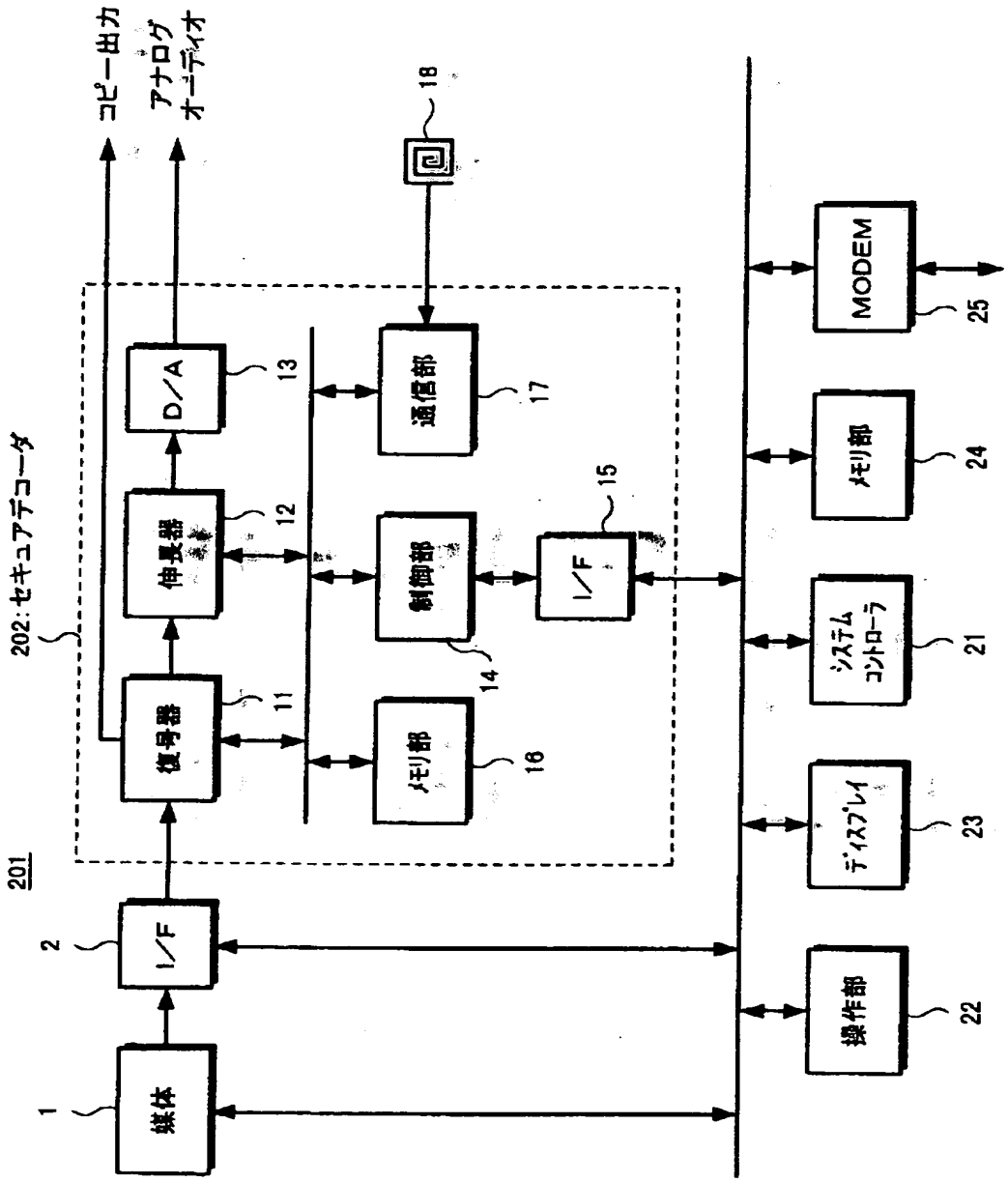
【図１】


103
著作権
管理機構
売上情報
分配金
110
104
109
A3
コンテンツ
供給事業者
売上情報
分配金
課金/決裁
センター
ユーザ
プリペイド
データ
101
A1
A5
A4
102
A6
A2, A7
コンテンツ
サーバ
認証/課金
サーバ
108
111
107
106
123
121
122
販売店
105

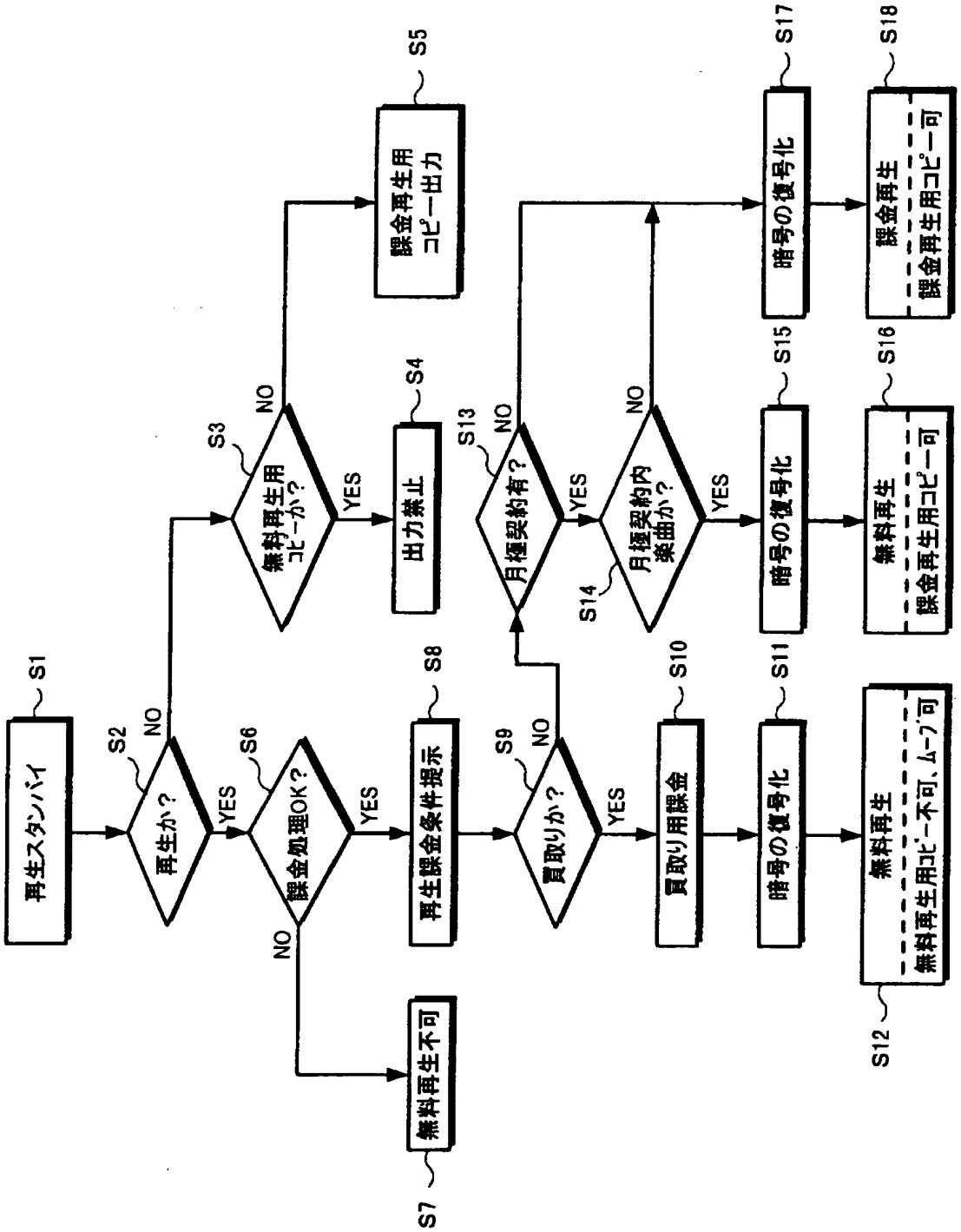
【図２】


課金／決裁センター
208
プリペイドデータ管理会社
205
著作権管理機構
103
コンテンツ供給事業者
101
プリペイドデータ販売機
206
プリペイドデータチャージャ
204
セキュアデコーダ
プレーヤ
202
201
207
203
再生ログ
プリペイドデータ
入金
管理委託
聴取料の支払い

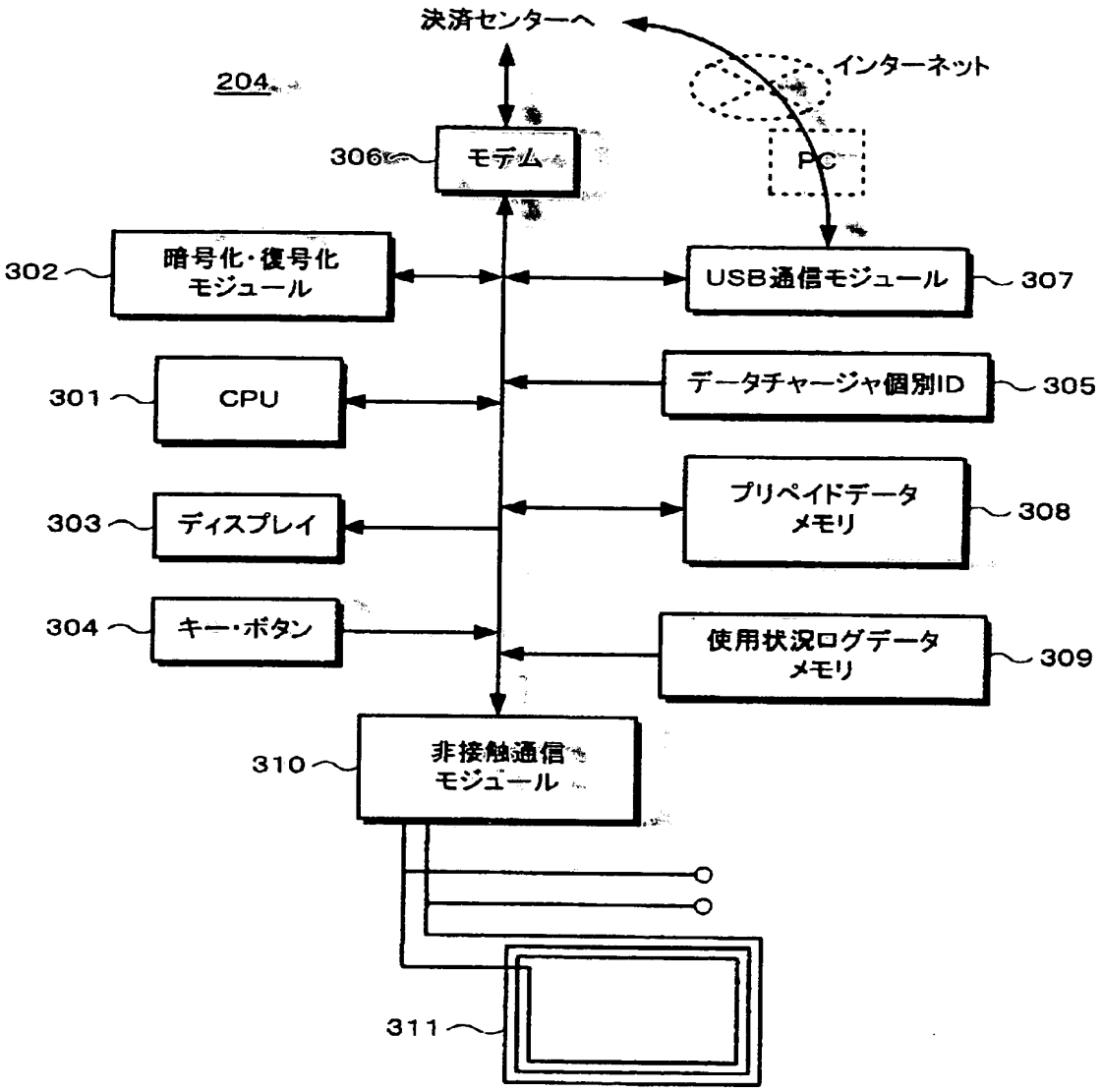
【図３】


コピー出力
アナログ
オーディオ
18
MODEM
25
D／A
13
通信部
17
メモリ部
24
伸長器
12
制御部
15
I／F
システム
コントローラ
21
復号器
11
メモリ部
14
16
ディスプレイ
23
202:セキュアデコーダ
201
I／F
2
操作部
22
媒体
1

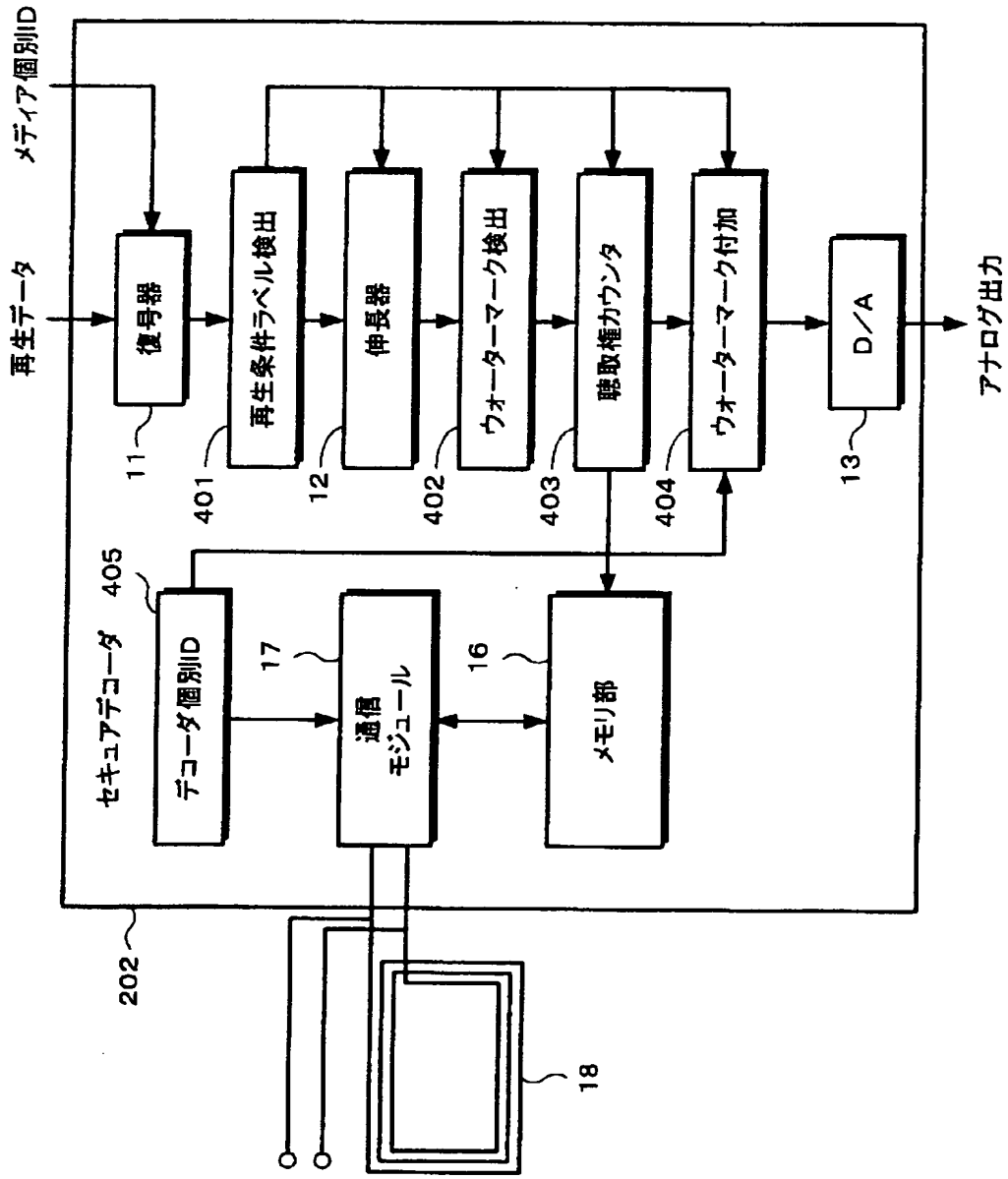
【図４】


再生スタンバイ
S1
再生か？
S2
NO
YES
無料再生用コピーか？
S3
NO
YES
課金再生用コピー出力
S5
出力禁止
S4
課金処理OK？
S6
NO
YES
無料再生不可
S7
再生課金条件提示
S8
買取りか？
S9
NO
YES
月極契約有？
S13
NO
YES
月極契約内楽曲か？
S14
NO
YES
買取り用課金
S10
暗号の復号化
S11
無料再生
無料再生用コピー不可、ムーブ可
S12
暗号の復号化
S15
無料再生
課金再生用コピー可
S16
暗号の復号化
S17
課金再生
課金再生用コピー可
S18

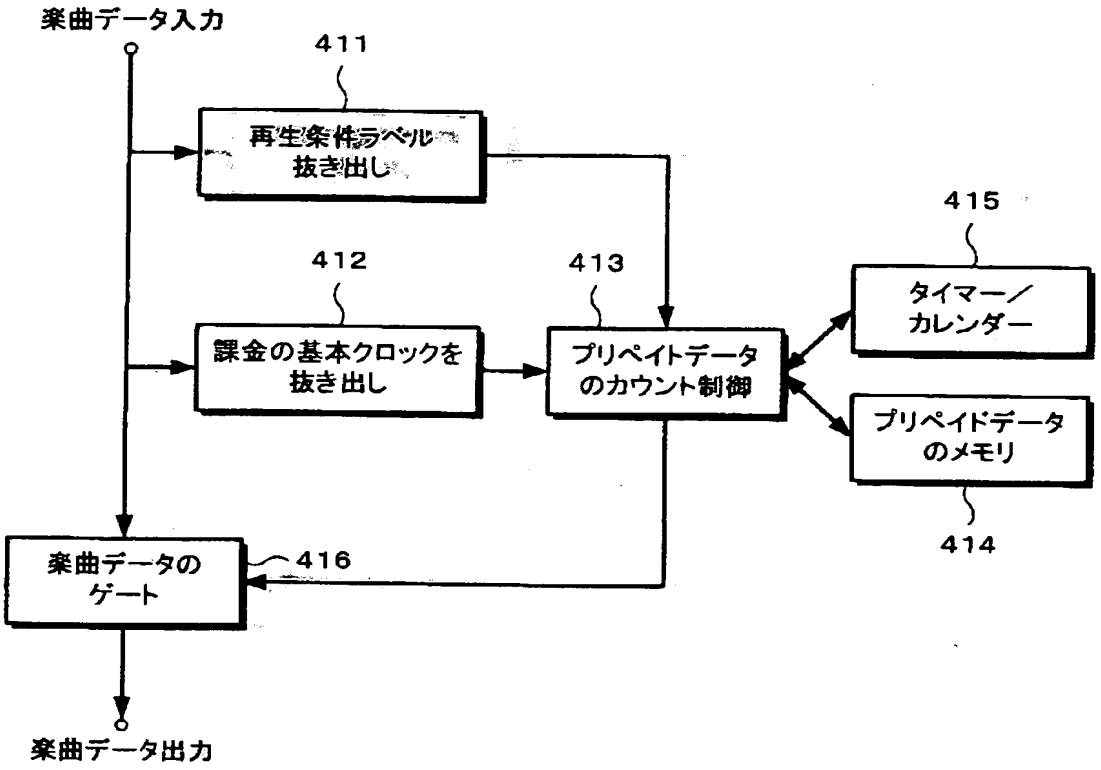
【図５】


決済センターへ
インターネット
204
306
モデム
PC
302
暗号化・復号化
モジュール
USB通信モジュール
307
301
CPU
データチャージャ個別ID
305
303
ディスプレイ
プリペイドデータ
メモリ
308
304
キー・ボタン
使用状況ログデータ
メモリ
309
310
非接触通信
モジュール
311

【図６】

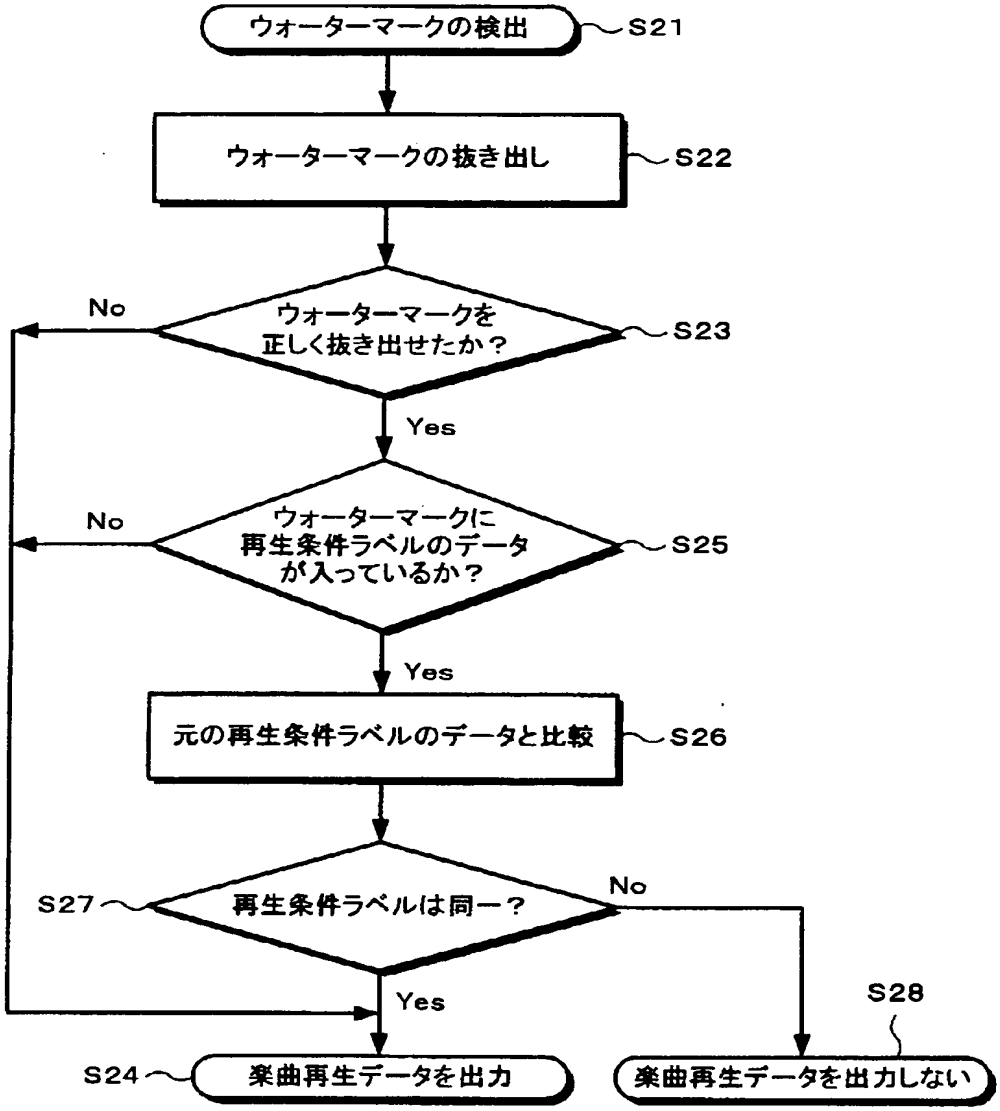

メディア個別ID
再生データ
復号器
再生条件ラベル検出
伸長器
ウォーターマーク検出
聴取権カウンタ
ウォーターマーク付加
D／A
アナログ出力
11
401
12
402
403
404
13
セキュアデコーダ
405
デコーダ個別ID
17
通信
モジュール
16
メモリ部
202
18

【図７】

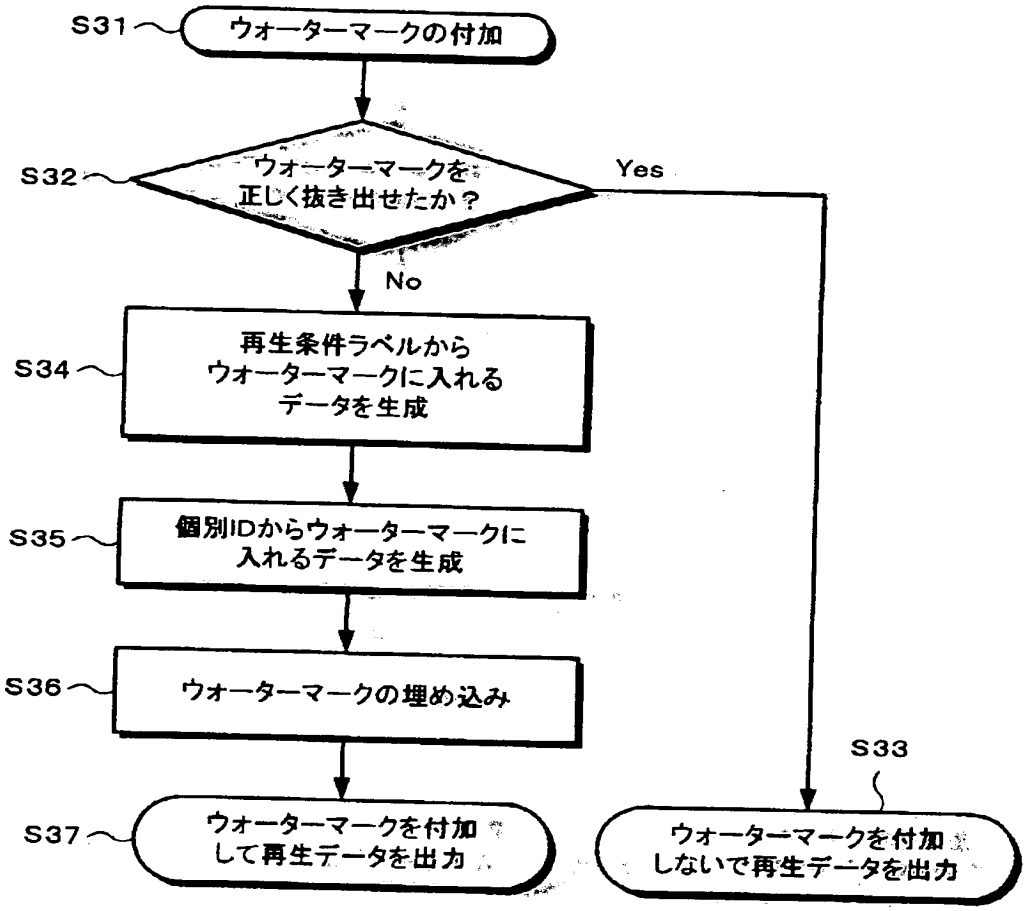


出証特２０００－３０６９９６３

【図８】


ウォーターマークの検出
S21
ウォーターマークの抜き出し
S22
ウォーターマークを
正しく抜き出せたか？
S23
No
Yes
ウォーターマークに
再生条件ラベルのデータ
が入っているか？
S25
No
Yes
元の再生条件ラベルのデータと比較
S26
再生条件ラベルは同一？
S27
No
Yes
S28
S24
楽曲再生データを出力
楽曲再生データを出力しない

【図９】


S31
ウォーターマークの付加
S32
ウォーターマークを正しく抜き出せたか？
Yes
No
S34
再生条件ラベルからウォーターマークに入れるデータを生成
S35
個別IDからウォーターマークに入れるデータを生成
S36
ウォーターマークの埋め込み
S37
ウォーターマークを付加して再生データを出力
S33
ウォーターマークを付加しないで再生データを出力

【書類名】　要約書

【要約】

【課題】　種々の課金処理条件に応じた課金処理を可能とし、視聴権データを安全にユーザに渡すことを可能とする。

【解決手段】　再生データが復号器１１に供給され、暗号が復号される。再生条件ラベル検出部４０１は、再生条件ラベルを検出する。伸長器１２では、圧縮符号化の復号がなされる。ウォーターマーク検出部４０２は、再生条件ラベルが改ざんされたか否かをチェックする。聴取権カウンタ４０３においては、再生データを復号する度に、聴取権データに対して変更を加える。メモリ部１６には、アンテナ１８と通信モジュール１７とによって、プリペイドデータチャージャ２０４から送信された聴取権データが格納される。通信モジュール１７内には、暗号化・復号化のモジュールが設けられている。ウォーターマーク付加部４０４において、出力されるデータに対してウォーターマークが付加され、Ｄ／Ａ変換器１３によってアナログ出力に変換され、外部へ出力される。

【選択図】　図６

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社